SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Valentina Plantak

FERMATOV DOPRINOS U TEORIJI BROJEVA

Diplomski rad

Voditelj rada:
Izv. prof. dr. sc. Zrinka Franušić

Zagreb, rujan, 2018.

Ovaj diplomski rad obranjen je dana ____________________ pred ispitnim povjerenstvom u sastavu:

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom _______________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Zahvaljujem se mentorici izv. prof. dr. sc. Zrinki Franušić na savjetima, potpori, strpljenju i vodstvu u izradi ovog diplomskog rada.
Posebnu zahvalnost iskazujem svojem zaručniku Patricku i najdražoj obitelji, posebno majci, ocu i sestrama, koji su me bezuvjetno podržavali, vjerovali u mene, ohrabrivali me i upućivali na pravi put. Hvala vam na vašoj ljubavi i pomoći, bez vas ne bih mogla ovo ostvariti!

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Teorija brojeva jedna je od najstarijih grana matematike kojom su se bavili najveći i najpoznatiji matematičari. Jedan od njih zasigurno je Pierre de Fermat, francuski matematičar amater iz prve polovice 17. stoljeća. On je uvelike pridonio razvoju teorije brojeva te ga se smatra ocem moderne teorije brojeva. Pierre de Fermat svoja otkrića nije objavljivao već su ona postala poznata preko njegove prepiske s drugim matematičarima te kroz njegove zabilješke na marginama Bachetovog prijevoda *Arithmetike*.

Ovaj diplomski rad posvećen je Fermatu i njegovim doprinosima u teoriji brojeva. Pregled tih doprinosa dan je u devet poglavlja. U prvom poglavlju ukratko je dana Fermatovova biografija.

Drugo poglavlje bavi se Fermatovim brojevima. To su brojevi oblika $F_m = 2^{2^m} + 1$, $m \in \mathbb{N}_0$. Fermat je pretpostavljao da su svi brojevi F_m prosti. No, Euler je pokazao da je broj F_5 složen i jedini do sada poznati prosti Fermatovi brojevi su F_0, F_1, F_2, F_3, F_4. Sluti se da su to i jedini. Mnoga pitanja vezana uz Fermatove brojeve su još i danas otvorena.

U trećem poglavlju opisana je Fermatova metoda faktorizacije. Fermat se bavio faktorizacijom velikih prirodnih brojeva. Fermatova metoda efikasna je samo kada su faktori broja kojeg treba faktorizirati blizu jedan drugome, odnosno kada je barem jedan djelitelj blizu broja $\sqrt{n}$.

Četvrto poglavlje posvećeno je jednoj od najvažnijih Fermatovih tvrdnji - *Malom Fermatovom teoremu*. Ovdje su dani iskaz i dokaz tog teorema, iako nije poznato je li ga sam Fermat dokazao. Službeno, prvi dokaz Malog Fermatovog teorema dao je Euler 1736. godine, a zatim ga je i generalizirao.

U sljedećem, petom, poglavlju opisujemo *Fermatovu metodu neprekidnog silaska* na koju je sam Fermat bio posebno ponosan. Ukratko, metodom se pokazuje da određena svojstva ili odnosi ne vrijede za prirodne brojeve ako je moguće konstruirati padajući niz prirodnih brojeva s tim svojstvom.

U šestom poglavlju *O zbroju kvadrata*, metodom neprekidnog silaska dokazujemo da se svaki prost broj oblika $4k + 1$ može prikazati kao zbroj kvadrata dva prirodna broja i to jedinstveno, do na poredak pribrojnika. Ta tvrdnja je još poznata pod nazivom *Fermatov teorem o zbroju dva kvadrata*. Navodimo i više srodnih rezultata koji su nastali pod utjecajem ove tvrdnje.

Sedmo poglavlje govori o poligonalnim brojevima. Fermat je uvidio da bi se prirodan broj mogao zapisati kao zbroj najviše tri trokutasta broja, kao zbroj najviše četiri kvadratna broja, kao zbroj najviše pet peterokutnih brojeva, odnosno općenito kao zbroj od najviše n n-terokutnih brojeva. Tvrdnju za $n = 3$ dokazao je Gauss (*Gaussov teorem o triagonalnim brojevima*), za $n = 4$ Lagrange (*Lagrangeov teorem o četiri kvadrata*), a za svaki n Cauchy.

Zadnja dva poglavlja opisuju Fermatov doprinos rješavanju diofantskih jednadžbi (Bachetov, Pellova) te priču o tvrdnji koja se dokazivala više od 350 godina. Riječ je o *Velikom Fermatovom teoremu* ili, kako ga još nazivaju, *Posljednjem Fermatovom teoremu* koji kaže da jednadžba

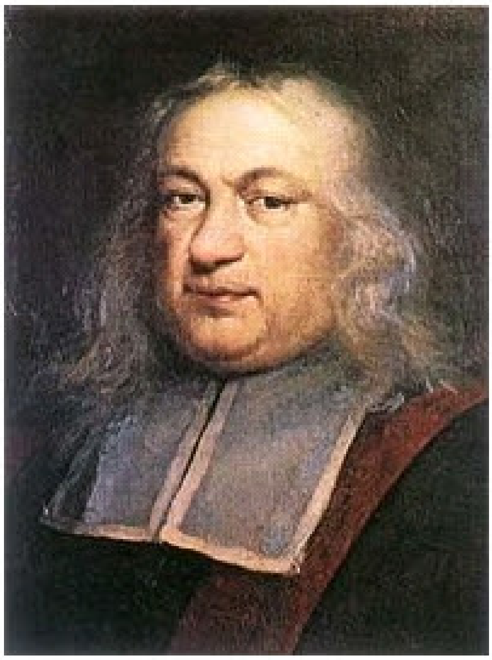
$$x^n + y^n = z^n$$

nema rješenja u skupu prirodnih brojeva za $n > 2$. Višegodišnji napori koji su ulagani za dokaz ove tvrdnje rezultirali su snažnim razvojem matematike, osobito algebarske teorije brojeva. Jedini Fermatov dokaz iz teorije brojeva je upravo dokaz Velikog Fermatovog teorema za $n = 4$.

Poglavlje 1

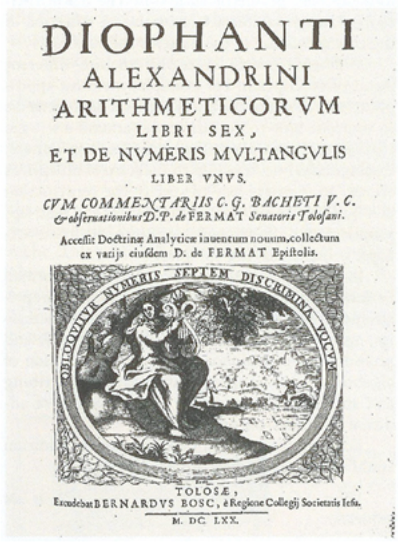
Pierre de Fermat

Pierre de Fermat bio je nedvojbeno najveći matematičar prve polovice 17. stoljeća. Rođen je 1604. godine u Beamontu, francuskom gradiću nedaleko Toulousa. Otac mu je bio uspješan trgovac kožom te je osim Pierra imao još jednog sina i dvije kćeri. Pierre Fermat je svoje školovanje započeo najprije kod kuće, a kasnije u lokalnom franjevačkom samostanu. Zatim je studirao pravo, najvjerojatnije u Toulousu. Tečno je govorio francuski, latinski, grčki, španjolski i talijanski jezik. 1631. godine Fermat je diplomirao pravo te je ubrzo nakon toga dobio mjesto savjetnika u francuskom parlamentu u Toulousu u kojem je brzo napredovao do najviše pozicije na kaznenom sudu. U to vrijeme promijenio je ime iz Pierre Fermata u Pierre de Fermat. Oženio se daljnjom rođakinjom, Louise Long s kojom je imao tri sina i dvije kćeri.



Slika 1.1: Pierre de Fermat

Iako je završio studij prava, Fermat se volio baviti matematikom, ali samo zbog užitka otkrivanja novih stvari, a ne zbog podizanja svoje reputacije. Fermat je napravio temeljne doprinose analitičkoj geometriji, analizi, vjerojatnosti i teoriji brojeva. Smatra ga se začetnikom infinitezimalnog računa. No, najveću matematičku strast Fermat je pokazivao prema teoriji brojeva i želio ju je prenijeti na druge.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Slika 1.2: Bachetov prijevod Arithmetike

Fermatov interes u teoriju brojeva potaknula je Diophantova *Arithmetika*. *Arithmetika* koja je prevedena na latinski jezik te koja je sadržavala *Bachetove*[1] komentare dospjela je 1630. godine u Fermatove ruke. Nekoliko vlastitih važnih otkrića Fermat je zapisao na marginama te knjige kao i svoje komentare i obrazloženja nekih Diophantovih rezultata.
Većina drugih Fermatovih rezultata postala su poznata kroz njegovu prepisku s tadašnjim vodećim znanstvenicima, ponajviše s Mersennom [2], Freniclom[3] i Carcavijem [4] koji su zagovarali širenje Fermatovog rada u široj znanstvenoj zajednici. Zanimljivo je da dokaze svojih rezultata Fermat nije davao u pismima niti ih je zapisivao na marginama knjige. Sve njegove tvrdnje, osim jedne, kasnije su se pokazale istinite. Jedan od glavnih Fermatovih ciljeva bio je zainteresirati matematičare svoga vremena (Huygensa[5], Pascala[6], Robervalla[7], Wallisa[8],...) za teoriju brojeva postavljajući pred njih izazovne probleme. O tome svjedoče i sljedeće riječi: *Pitanja (problemi) ovakve vrste nisu inferiorni u odnosu na poznata pitanja (probleme) u geometriji s obzirom na ljepotu, težinu ili metodu dokaza.*

[1]Claude Gaspard Bachet de Méziriac (1591.-1638.), francuski matematičar, lingvist i pjesnik
[2]Marin Mersenne (1588.-1648.), francuski svećenik, filozof i matematičar
[3]Bernard Frenicle de Bessy (1604.-1674.), francuski matematičar
[4]Pierre de Carcavi (1603.-1684.), francuski matematičar
[5]Christian Huygens (1629.-1695.), nizozemski astronom, fizičar i matematičar
[6]Blaise Pascal (1623.-1662.), francuski matematičar
[7]Gilles Personne de Roberval (1602.-1675.), francuski matematičar
[8]John Wallis (1616.-1703.), engleski matematičar i teolog

No, u tome ipak nije imao uspjeha kakvog je priželjkivao. Matematičari su pokazali ozbiljniju zainteresiranost za teoriju brojeva tek nakon Eulera, sto godina kasnije.

Pierre de Fermat umro je 9. siječnja 1665. godine u Castresu te je pokopan 12. siječnja. Jedan od njegovih sinova, Clement Samuel objavio je 1670. godine očeve komentare koji su se nalazili na marginama *Arithmetike*. Osim ovog djela sačuvano je i nekoliko kolekcija Fermatovih pisama.

Poglavlje 2

Fermatovi brojevi

Fermat je proučavao proste brojeve oblika $2^n - 1$, $n \in \mathbb{N}$, a njima se posebno bavio Marin Mersenne pa su njemu u čast i dobili ime *Mersenneovi brojevi*. To je sigurno utjecalo na malu modifikaciju problema pa se Fermat počeo zanimati za proste brojeve oblika

$$2^n + 1,$$

$n \in \mathbb{N}$. U nekoliko navrata Fermat je u svojoj prepisci s drugim matematičarima tvrdio da su brojevi $2^n + 1, n \in \mathbb{N}$ prosti ako je

$$n = 2^m,\ m \in \{0, 1, 2, 3, \ldots\}.$$

Brojevi oblika

$$F_m = 2^{2^m} + 1, \tag{2.1}$$

$m \in \mathbb{N}_0$ su kasnije nazvani *Fermatovi brojevi*. Dakle, Fermatova pretpostavka bila je da su svi brojevi oblika (2.1) prosti. Tu je hipotezu podkrijepio činjenicom da se za $m = 0, 1, 2, 3, 4$ dobivaju brojevi

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

koji su uistinu prosti. Sam Fermat nikada nije tvrdio da ima dokaz svoje slutnje. Sljedeći broj tog oblika, za $m = 5$, je deseteroznamenkasti broj 4 294 967 297 i za njega nije mogao utvrditi je li prost ili složen. No, 1732. godine Euler je pokazao da je broj F_5 složen tako što je ustanovio da je djeljiv s 641, odnosno

$$F_5 = 641 \cdot 6700417.$$

Štoviše, Euler je 1873. pokazao da ako je F_m složen, onda je svaki njegov djelitelj oblika $k \cdot 2^{m+1} + 1$, $k \in \mathbb{N}$. Nekako u to vrijeme pokazalo se i da je $F_6 = 18\,446\,744\,073\,709\,551\,617$ složen broj,

$$F_6 = 274\,177 \cdot 67\,280\,421\,310\,721.$$

To je u svakom slučaju opovrgnulo Fermatovu slutnju da je svaki broj oblika (2.1) prost. Štoviše, do sada osim prvih pet Fermatovih prostih brojeva nije pronađen niti jedan drugi pa se sluti da su svi F_m, $m > 4$ složeni. Štoviše, niti na jedno od sljedećih pitanja ne možemo dati pouzdan odgovor:

- *Postoji li bekonačno Fermatovih prostih brojeva?*
- *Postoji li bekonačno Fermatovih složenih brojeva?*
- *Jesu li svi Fermatovi složeni brojevi kvadratno slobodni?*

Neki vjerojatnosni argumenti za procjenu broja Fermatovih prostih brojeva ukazuju na oprečne tvrdnje, po nekima bi ih moglo biti beskonačno, a po nekima konačno (najviše $2/\ln 2$).

Nije sasvim slučajno, zašto je Fermat smatrao da su brojevi oblika (2.1) prosti. Vrijedi, naime, sljedeća tvrdnja.

Teorem 2.1. *Ako je $2^k + 1$ neparan prost broj, tada je k potencija broja 2, odnosno oblika 2^n za $n \in \mathbb{N}_0$.*

Dokaz. Pretpostavimo da k nije potencija broja 2. Tada postoji neparan prost broj p koji dijeli k, odnosno

$$k = mp,\ m \in \mathbb{N},\ m < k.$$

No, tada $2^m + 1$ dijeli $2^{mp} + 1$. Zaista, kako općenito vrijedi $(a - b) \mid (a^m - b^m)$, za $a = 2^m$, $b = -1$ dobivamo navedenu relaciju. Stoga pretpostavka da k ima neparnog prostog djelitelja povlači da je broj $2^{mp} + 1$ složen. □

Moguće je da je sam Fermat možda pomislio da vrijedi obrat prethodne tvrdnje, a u to ga je dodatno uvjerila i činjenica da prvih nekoliko Fermatovih brojeva jesu prosti.

Danas znamo i kojeg su oblika djelitelji Fermatovih složenih brojeva. Édouard Lucas[1] je pokazao sljedeće:

Teorem 2.2. *Ako je p prosti djelitelj od F_n, $n > 1$, onda je p oblika*

$$k2^{n+2} + 1.$$

[1] François Édouard Anatole Lucas (1842.-1891.), francuski matematičar

Do 1796. godine Fermatovi brojevi su najvjerojatnije bili samo matematička znatiželja. Interes za Fermatove brojeve drastično se povećao kada je njemački matematičar Carl Friedrich Gauss[2] prilično neočekivano otkrio teorem koji izražava zanimljivu povezanost između euklidskih konstrukcija pravilnih poligona i Fermatovih brojeva. On je pokazao da se pravilni n-terokut može konstruirati za $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots$. Preciznije, Gauss je dokazao da postoje euklidske konstrukcije pravilnih n-terokuta ako

$$n = 2^i \cdot F_{m_1} F_{m_2} F_{m_3} \cdots F_{m_j},$$

gdje su $n \geq 3, i \geq 0, j \geq 0$ i F_{m_1}, F_{m_2}, ...,F_{m_j} Fermatovi prosti brojevi ili 1.

[2] Carl Friedrich Gauss (1777.-1855.), njemački matematičar i fizičar

Poglavlje 3

Fermatova metoda faktorizacije

Pierre de Fermat bavio se problemom faktorizacije velikih prirodnih brojeva. Taj problem aktualan je još i danas. 1643. godine poslao je pismo Mersennu u kojem od njega traži da mu zada neki veliki broj kojega će tada on ispitati i provjeriti je li taj broj prost ili složen. Ako je složen, tada će mu napisati faktore čiji umožak daje taj broj. U tom istom pismu Fermat je dao odgovor na to kako će doći do faktora složenog broja. Ta metoda je kasnije postala poznata kao *Fermatova metoda faktorizacije*, a temelji se na jednostavnoj činjenici da broj koji možemo prikazati kao razliku kvadrata dva prirodna broja, možemo i faktorizirati. Naime,

$$n = x^2 - y^2 = (x - y)(x + y).$$

Ova faktorizacija neće biti od posebnog interesa ako je $x - y = 1$, odnosno $n = n \cdot 1$. Nadalje, jednostavno se može uočiti da svaki neparan broj veći od 1 možemo prikazati kao razliku kvadrata dva prirodna broja. Ako je n neparan broj i $n = ab$, gdje su $a, b \in \mathbb{N}$ također neparni, tada za

$$x = \frac{a+b}{2}, y = \frac{a-b}{2}$$

vrijedi

$$n = x^2 - y^2.$$

Na drugi način, ako je $n > 1$ neparan, onda postoji $m \in \mathbb{N}$ takav da je $n = 2m + 1$. Očito je

$$n = 2m + 1 = (m + 1)^2 - m^2.$$

Fermatova metoda faktorizacije:
Pretpostavimo da je $n > 1$ neparan broj.

- Ako je n kvadrat nekog broja a, tada smo gotovi, $n = a \cdot a$.

- Ako n nije potpun kvadrat, definiramo

  $$a = \lfloor \sqrt{n} \rfloor,$$

  gdje smo s $\lfloor \cdot \rfloor$ označili funkciju najveće cijelo. Očito, $a^2 < x^2 < (a+1)^2$. Neka je

  $$x_1 = (a+1)^2 - n.$$

  Ako je x_1 kvadrat nekog broja b, onda smo gotovi jer iz $(a+1)^2 - n = b^2$ slijedi

  $$n = a^2 - b^2 = (a+1-b)(a+1+b).$$

- Ako x_1 nije potpun kvadrat, tražimo sljedećeg kandidata za puni kvadrat,

  $$x_2 = (a+2)^2 - n.$$

  Ako je x_2 potpun kvadrat, onda smo gotovi jer $n = (a+2-b)(a+2+b)$.

- Ako x_2 nije puni kvadrat, povećamo broj a za 3 i ponavljamo postupak.
  Budući da znamo da se n može prikazati kao razlika kvadrata dva prirodna broja, algoritam završava nakon konačno mnogo koraka. Stoga, postoji $m \in \mathbb{N}$ za koji je $x_m = (a+m)^2 - n$ kvadrat prirodnog broja b pa je

  $$n = (a+m)^2 - b^2 = (a+m-b)(a+m+b).$$

Fermatova metoda faktorizacije efikasna je samo kada su faktori broja kojeg se treba faktorizirati blizu jedan drugome.

Primjer 3.1. Faktorizirat ćemo broj $n = 957$ pomoću Fermatove metode.

- Kako n nije potpuni kvadrat, stavljamo $a = \lfloor \sqrt{957} \rfloor = 30$.
- $x_1 = (30+1)^2 - 957 = 4$ je potpun kvadrat pa je

  $$957 = (31-2)(31+2) = 29 \cdot 33.$$

Primjer 3.2. Ovdje ćemo vidjeti kako Fermatova metoda funkcionira na prostom broju $n = 13$.

- $a = \lfloor \sqrt{13} \rfloor = 3$,
- $x_1 = (3+1)^2 - 13 = 3 \neq \square$,
- $x_2 = (3+2)^2 - 13 = 12 \neq \square$,

- $x_3 = (3+3)^2 - 13 = 23 \neq \square$,
- $x_4 = (3+4)^2 - 13 = 36 = 6^2$ pa je $13 = (7-6)(7+6) = 1 \cdot 13$.

Fermatova metoda faktorizacije ima najveći broj koraka u slučaju kada se traži faktorizacija prostog broja (Primjer 3.2). U tom slučaju algoritam je dovršen tek kada je jedan od faktora broj 1, a drugi faktor je sam taj broj. Odnosno,

$$a + m - b = 1, \; a + m + b = n.$$

Zbrajanjem ovih jednakosti dobivamo $2(a+m) = n+1$, pa vrijedi sljedeća ocjena na broj koraka Fermatove metode:

$$m \leq \frac{1}{2}(n+1) - \lfloor \sqrt{n} \rfloor.$$

Stoga je ova metoda neučinkovita za velike složene brojeve, osim u slučaju kada broj n ima djelitelja blizu $\sqrt{n}$.

Iako smo ustanovili da je Fermatova metoda faktorizacije učinkovita samo u specijalnom slučaju, na njenoj ideji se bazira jedan od najpoznatijih i najučinkovitijih algoritama za faktorizaciju, *algoritam kvadratnog sita*.

Poglavlje 4

Mali Fermatov teorem

Smatra se da su Kinezi već oko 500.g.pr.Kr. znali da je broj $2^p - 2$ djeljiv prostim brojem p. Tu činjenicu ponovo je otkrio Fermat kada je proučavao savršene brojeve. Nedugo nakon toga Fermat je došao do jedne od njegovih najvažnijih doprinosa u teoriji brojeva, a to je tvrdnja koju danas poznajemo pod nazivom *Mali Fermatov teorem*. Fermat je svoju tvrdnju iskazivao na više različitih načina. Tako je 1640. godine u pismu Frenicleu stajalo:

Za dani prost broj p i bilo koji geometrijski niz $1, a, a^2, \ldots,$ p dijeli $a^n - 1$ pri čemu n dijeli $p - 1$.

Danas je uobičajeno tvrdnju iskazati na sljedeći način.

Teorem 4.1 (Mali Fermatov teorem)**.** *Ako je a prirodan broj i p prost broj, tada je broj $a^p - a$ djeljiv brojem p.*

Nakon što je Gauss uveo oznaku za kongruenciju, tvrdnju Malog Fermatovog teorema zapisujemo kao:

Za prirodan broj a i prost broj p vrijedi

$$a^p \equiv a \pmod{p}.$$

Uočimo da ako p ne dijeli a, onda iz činjenice da p dijeli $a^p - a = a(a^{p-1} - 1)$ slijedi da p dijeli $a^{p-1} - 1$. Obrat je očigledan. Stoga je česta i sljedeća varijanta iskaza:

Za prirodan broj a i prost broj p koji ne dijeli a vrijedi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Smatra se da je Fermat do svoga zaključka došao baveći se savršenim brojevima, odnosno brojevima koji su jednaki zbroju svojih djelitelja osim sebe samog. Još je Euklid pokazao da ako je $2^n - 1$ prost, onda je $2^{n-1}(2^n - 1)$ savršen broj. Stoga su ga zanimali djelitelji broja $2^n - 1$. Nadalje, Fermat je bio upoznat i s rezultatom starih Kineza (500 godina pr. Kr.) da p dijeli $2^p - 2$, što je zapravo specijalan slučaj Malog Fermatovog teorema za $a = 2$. Nije poznato je li Fermat znao dokazati svoju tvrdnju i stoga se prihvaća da je Euler[1] bio taj koji ga je prvi dokazao. Prvi Eulerov dokaz koji koristi binomne koeficijente objavljen je 1736. godine. Euler je dao još nekoliko dokaza, te poopćio tvdnju. Mi ćemo izložiti jedan od elegantnijih dokaza.

Dokaz Teorema 4.1. Ako p dijeli a, onda p očito dijeli $a^p - a$. Neka su p i a relativno prosti brojevi. Pokazat ćemo da tada p dijeli $a^{p-1} - 1$. Promotrimo konačan niz brojeva

$$a, 2a, 3a, \ldots, (p-1)a. \tag{4.1}$$

Dijeljenjem dva broja ia i ja, $1 \leq j < i \leq p$ brojem p ne možemo dobiti isti ostatak zato što bi tada broj p dijelio broj $a(i - j)$, a to je u kontradikciji s pretpostavkom da su brojevi p i a relativno prosti. Stoga, niz (4.1) daje $p - 1$ različitih ostataka pri dijeljenju s brojem p i to su

$$1, 2, \ldots, p-1. \tag{4.2}$$

Zaključujemo da je umnožak elemenata u (4.1) kongruentan modulo p umnošku elemenata u (4.2),

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}. \tag{4.3}$$

Kako p ne dijeli $(p - 1)!$ slijedi da

$$a^{p-1} \equiv 1 \pmod{p}$$

što je i trebalo dokazati. □

Obrat Malog Fermatovog teorema ne vrijedi, što znači da iz pretpostavke da p dijeli broj $a^{p-1} - 1$ ne možemo zaključiti da je p prost. To je najlakše pokazati konstrukcijom konkretnog protuprimjera.

Primjer 4.2. Neka je $a = 2$ i $p = 341 = 31 \cdot 11$. Iz $2^{10} \equiv 1 \pmod{341}$ slijedi da je $2^{340} \equiv 1 \pmod{341}$. No, 341 je složen broj. Za takve brojeve kažemo da su Fermatovi pseudoprosti u bazi 2.

Općenito, za složen broj n koji je relativno prost s a i vrijedi

$$a^{n-1} \equiv 1 \pmod{n} \tag{4.4}$$

kažemo da je *Fermatov pseudoprost u bazi a*. Ako broj n zadovoljava relaciju (4.4) za različite vrijednosti baze, onda je *vjerojatno* prost broj. Upravo na tome se zasniva tzv.

[1]Leonhard Euler(1707.-1783.), švicarski matematičar, fizičar, astronom, logičar i inžinjer

Fermatov vjerojatnostni test prostosti. Kao što i sam naziv kaže on je *vjerojatnostan* i ne daje egzaktan odgovor kakav mogu dati samo deterministički testovi. No, oni su, za razliku od ovog vjerojatnostnog, skupi, odnosno traju puno duže. Zato se u praksi kombiniraju vjerojatnostni i determinstički testovi.

Zanimljivost u vezi Fermatovog vjerojatnostnog testa jest činjenica da postoje složeni brojevi koji *prolaze* testiranje za svaku bazu. Složen broj koji je Fermatov pseudoprost u svakoj bazi naziva se *Carmichaelov broj*. Najmanji Carmichaelov broj je $561 = 3 \cdot 11 \cdot 17$ a dokazano je da ih postoji beskonačno mnogo.

Već smo spomenuli da je Euler dokazao Teorem 4.1 na više načina. U jednom od načina uočio je važnost funkcije koja svakom prirodnom broju n pridružuje broj brojeva u nizu $1, 2, \ldots, n$ s kojima je n relativno prost. Ta se funkcija danas naziva *Eulerova funkcija* i označava s φ. Poopćenje Malog Fermatovog teorema glasi:

Teorem 4.3 (Eulerov teorem)**.** *Neka je n prirodan broj i a cijeli broj koji je relativno prost s n. Tada je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Kako je $\varphi(p) = p - 1$ za p prost broj, prethodni teorem uistinu je generalizacija MFT-a.

Poglavlje 5

Fermatova metoda neprekidnog silaska

Fermat je u svojim pismima (Carcaviju, Huygensu) pisao da je otkrio vrlo jednostavnu metodu pomoću koje se mogu dokazati teške propozicije. Također je napisao da ju je nazvao *metoda neprekidnog silaska*. Možemo reći da je to specifičan oblik principa matematičke indukcije koja omogućava rješavanje mnogih izazovnih problema iz teorije brojeva, osobito iz područja diofantskih jednadžbi. Metoda se bazira na činjenici da u skupu prirodnih brojeva postoji samo konačno mnogo onih koji su manji od zadanog broja. Drugim riječima, ne postoji strogo padajući niz prirodnih brojeva. Iako je i Euklid koristio ovu ideju, metoda neprekidnog silaska pripisuje se Fermatu jer ju je eksplicitno opisao.

Metoda neprekidnog silaska:
Neka je $n > 1$ prirodan broj i pretpostavimo da n zadovoljava svojstvo P. Ako iz pretpostavke možemo dokazati egzistenciju prirodnog broja $n_1 < n$ koji zadovoljava svojstvo P, onda bi postupak mogli ponoviti u nedogled, $n > n_1 > n_2 > \cdots$, što je u kontradikciji s činjenicom da postoji samo konačno mnogo prirodnih brojeva manjih od n. Stoga svojstvo P može vrijediti, eventualno, za $n = 1$.

Postoji i varijanta ove metode u kojoj pretpostavimo da je $n > 1$ najmanji prirodan broj koji zadovoljava svojstvo P. Ako se dokaže postojanje prirodnog $n_1 < n$ koji zadovoljava svojstvo P, onda je to kontradikcija s pretpostavkom, pa slijedi da je $n = 1$.

Jednostavna ideja metode neprekidnih silazaka može se implementirati na sljedećem primjeru:

Primjer 5.1. *Pokažimo da je $\sqrt{3}$ iracionalan broj.*

Pretpostavimo suprotno, tj. pretpostavimo da je $\sqrt{3}$ racionalan broj. Tada ga možemo zapisati u obliku razlomka, odnosno

$$\sqrt{3} = \frac{p}{q}, \tag{5.1}$$

gdje su $p, q \in \mathbb{N}$. Kvadriranjem 5.1 dobivamo

$$3 = \frac{p^2}{q^2}, \tag{5.2}$$

odnosno

$$3q^2 = p^2. \tag{5.3}$$

Iz (6.6) slijedi da $3 \mid p^2$ te otuda $3 \mid p$. Dakle, $p = 3p_1$, $p_1 \in \mathbb{N}$. Uvrštavanjem u 6.6 dobivamo:

$$3q^2 = 9p_1^2,$$

odnosno

$$q^2 = 3p_1^2.$$

Otuda slijedi $3 \mid q$, odnosno $q = 3q_1$. Dakle, pronašli smo $0 < p_1 < p$, $0 < q_1 < q$ za koje je

$$\sqrt{3} = \frac{p_1}{q_1}.$$

Očito je da bismo cijeli postupak mogli ponavljati u nedogled što je nemoguće pa je naša pretpostavka o tome da je $\sqrt{3}$ racionalan broj kriva.

□

Fermatovom metodom silaska pokazat ćemo i sljedeću vrlo primjenjivanu tvrdnju.

Propozicija 5.2. *Neka su v i w relativno prosti prirodni brojevi i vw je potpuni kvadrat. Tada su v i w potpuni kvadrati.*

Dokaz. Neka su $u, v, w \in \mathbb{N}$ za koje vrijedi

$$v > 1,\ v \neq \square,\ (v, w) = 1,\ vw = u^2. \tag{5.4}$$

Kako je $v > 1$, postoji prost broj p takav da $p \mid v$ pa je $v = pk$, za neki $k \in \mathbb{N}$. Otuda slijedi

$$pkw = u^2 \ \Rightarrow\ p \mid u^2 \ \Rightarrow\ p \mid u.$$

Stoga je $u = pm$ za $m \in \mathbb{N}$ te

$$pkw = p^2m^2 \ \Rightarrow\ kw = pm^2 \ \Rightarrow\ p \mid kw.$$

Budući da p ne može dijeliti w jer bi to značilo da je $(v, w) \geq p$, pa p mora dijeliti k. Neka je $k = pv_1$, $v_1 \in \mathbb{N}$. Sada

$$pv_1w = pm^2 \ \Rightarrow\ v_1w = m^2.$$

Stoga smo pokazali egzistenciju broja v_1 za kojeg vrijedi

$$v_1 < v, \ (v_1, w) = 1, \ v_1 w = m^2.$$

Ako bi pretpostavili da v_1 nije potpuni kvadrat, dobili bi $v_2 < v_1$, odnosno nastavljajući dalje dobili bi niz $v > v_1 > v_2 > v_3 \ldots$ koji zadovoljava (5.4) što nije moguće. Stoga je pretpostavka da v nije potpuni kvadrat nije točna. □

Za kraj napomenimo da je Fermat bio izuzetno ponosan na svoju metodu dokaza. U dugom pismu napisanom pred kraj života navodi sva svoja postignuća iz teorije brojeva te izjavljuje da je ona implementirana u gotovo svim njegovim dokazima.

Poglavlje 6

O zbroju kvadrata

U ovom poglavlju govorimo najviše o Fermatovom teoremu o zbroju dva kvadrata. Za početak napomenimo da ćemo pod pojmom *zbroj dva kvadrata* misliti na zbroj kvadrata dva cijela broja. Iz tog razloga i brojeve koji su puni kvadrati ubrajamo među one koji se mogu prikazati kao zbroj dva kvadrata, $a^2 = a^2 + 0^2$.

U dokazu Fermatovog teorema o zbroju dva kvadrata koristi se metoda neprekidnog silaska opisana u prethodnom poglavlju.

6.1 Zbroj dva kvadrata

U *Arithmetici* Diophant je zapisao svoje zapažanje da je produkt dvaju brojeva, od kojih je svaki zbroj dva kvadrata, jednak zbroju dva kvadrata. Danas tu činjenicu jednostavno vidimo iz sljedećeg identiteta:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \tag{6.1}$$

Neki smatraju da je upravo to potaknulo Fermata da postavi pitanje:

Koji su sve brojevi jednaki zbroju dva kvadrata?

Fermat je lako ustanovio da je za to dovoljno dati odgovor na sljedeće pitanje:

Koji su sve prosti brojevi jednaki zbroju dva kvadrata?

Naime, svaki složen prirodan broj jednak je umnošku prostih. Nadalje, identitet (6.1) se lako može poopćiti za umnožak konačno mnogo kvadrata, odnosno umnožak proizvoljno mnogo brojeva, od kojih je svaki jednak zbroju dva kvadrata, jest zbroj dva kvadrata.

Najmanji prost broj 2 je očito prikaziv kao zbroj kvadrata, $2 = 1^2 + 1^2$. Za neparne proste brojeve oblika $4k + 3$ vrijedi sljedeća tvrdnja:

Propozicija 6.1. *Prost broj oblika* $4k + 3$ *ne može se prikazati kao zbroj dva kvadrata.*

Dokaz. Kvadrat cijelog broja kongruentan je 0 ili 1 modulo 4. Stoga je zbroj kvadrata kongruentan 0, 1 ili 2 modulo 4, odnosno različit od 3 modulo 4. □

Ovu tvrdnju (bez dokaza) Fermat je iznio u pismu 1640. godine Roberval, a dokazao ju je 1742. godine Euler.

Za neparne proste brojeve oblika $4k + 1$ vrijedi sasvim drugačija tvrdnja:

Teorem 6.2. *Svaki prost broj oblika* $4k + 1$ *može se jedinstveno zapisati kao zbroj dva kvadrata.*

Prethodna tvrdnja je poznata pod nazivom *Fermatov teorem o zbroju dva kvadrata*, a Fermat ju je iskazao 1640. godine iako je bila i ranije poznata Albertu Girardu[1]. U pismu Huygensu Fermat je dao indikacije kako je on dokazao tvrdnju o zbroju dva kvadrata, ali taj dokaz nije nigdje objavio. Fermat je u tom pismu napisao da je pritom koristio svoju metodu neprekidnog silaska. Za prvi službeni dokaz ove tvrdnje smatramo onaj Eulerov iz 1747. godine. Postoji još nekoliko dokaza ove tvrdnje koji su proizašli razvojem nekih matematičkih grana (algebra, topologija). Mi ćemo tvrdnju pokazati koristeći elementarnu teoriju brojeva i metodu silaska.

Propozicija 6.3. *Neka je* p *prost broj oblika* $4k + 1$. *Tada postoje* $x, y \in \mathbb{N}$, $(x, y) = 1$, *takvi da* p *dijeli* $x^2 + y^2$.

Dokaz. Prema Wilsonovom teoremu je

$$(p-1)! \equiv -1 \pmod{p}. \tag{6.2}$$

za svaki prost broj p. Kako je

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdots (p-2) \cdot (p-1) \\ &\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 \pmod{p},\end{aligned}$$

za $p = 4k + 1$ i $x = \left(\frac{p-1}{2}\right)!$ je

$$(p-1)! \equiv x^2 \pmod{p}.$$

[1] Albert Girard (1595.-1632.), francuski matematičar

Sada zbog (6.2) dobivamo

$$-1 \equiv x^2 \pmod{p}.$$

Dakle, za $x = \left(\frac{p-1}{2}\right)!$ i $y = 1$, zadovoljeno je $(x, y) = 1$ i

$$p \mid x^2 + y^2.$$

□

U dokazu sljedeće propozicije primijenit ćemo Fermatovu metodu silaska.

Propozicija 6.4. *Ako prost broj p dijeli sumu dva kvadrata $x^2 + y^2$, $(x, y) = 1$, onda je p i sam suma dva kvadrata.*

Dokaz. Budući da

$$p \mid x^2 + y^2,$$

postoji $k \in \mathbb{N}$ takav da je

$$pk = x^2 + y^2. \tag{6.3}$$

Ako je $k = 1$, onda tvrdnja vrijedi. Zato pretpostavimo da je $k > 1$. Nadalje, možemo pretpostaviti da je $k < \frac{p}{2}$. Zaista, ako bi $k > \frac{p}{2}$, onda bi za $a, b \in \mathbb{Z}$, $|a|, |b| \leq \frac{p}{2}$ takve da je

$$x \equiv a \pmod{p}, \; y \equiv b \pmod{p}$$

vrijedilo

$$a^2 + b^2 \equiv x^2 + y^2 \equiv 0 \pmod{p}.$$

Kako je

$$a^2 + b^2 \leq \frac{p^2}{4} + \frac{p^2}{4} = \frac{p^2}{2} = p \cdot \frac{p}{2}.$$

Stoga smo pronašli $a, b \in \mathbb{Z}$, $(a, b) = 1$ takve da je

$$pk' = a^2 + b^2$$

i $k' < \frac{p}{2}$.

Nastavimo dalje dokaz uz prepostavku da je $1 < k < \frac{p}{2}$ i da vrijedi (6.3) za $(x, y) = 1$. Neka su $u, v \in \mathbb{Z}$, $|u|, |v| \leq \frac{k}{2}$ za koje je

$$x \equiv u \pmod{k}, \; y \equiv v \pmod{k}.$$

Tada je

$$u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{k}.$$

To znači da postoji $l \in \mathbb{N}$ takav da je

$$u^2 + v^2 = kl.$$

Nadalje, iz

$$u^2 + v^2 \le \frac{k^2}{4} + \frac{k^2}{4} = \frac{k^2}{2} = k \cdot \frac{k}{2}$$

slijedi da je $1 \le l \le \frac{k}{2}$.

Primjenimo identitet (6.1) na umnožak kvadrata $x^2 + y^2$ i $u^2 + v^2$:

$$(x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2.$$

S druge strane je

$$(x^2 + y^2)(u^2 + v^2) = pk^2 l,$$

odnosno

$$(xu + yv)^2 + (xv - yu)^2 = pk^2 l. \tag{6.4}$$

Uočimo da je

$$xu + yv \equiv u^2 + v^2 \equiv 0 \pmod{k},$$

$$xv - yu \equiv uv - vu = 0 \pmod{k}.$$

Stoga postoje $x_1, y_1 \in \mathbb{Z}$, $(x_1, y_1) = 1$, $d \in \mathbb{N}$ takvi da

$$xu + yv = x_1 dk, \; xv - yu = y_1 dk.$$

Uvrštavanjem u (6.4) dobivamo

$$(x_1 dk)^2 + (y_1 dk)^2 = pk^2 l,$$

te nakon skraćivanja s k^2 i dijeljenja s d^2:

$$x_1^2 + y_1^2 = p\frac{l}{d^2}.$$

Prethodnom jednakošću smo upravo pokazali da postoji $k_1 \in \mathbb{N}$ za koji je $k_1 = \frac{l}{d^2} \le l \le \frac{k}{2} < k$ i relativno prosti cijeli brojevi x_1 i y_1 takvi da je

$$pk_1 = x_1^2 + y_1^2.$$

Metodom neprekidnih silazaka možemo zaključiti da nakon konačno mnogo koraka dobivamo $k_i = 1$ i

$$p = x_i^2 + y_i^2.$$

□

Posljedica propozicija 6.3 i 6.4 jest tvrdnja da se prosti brojevi oblika $4k + 1$ mogu prikazati kao zbroj dva kvadrata. Još samo ostaje za pokazati jedinstvenost tog prikaza. Prije nego što to pokažemo pokušajmo iskoristiti metodu iz dokaza Propozicije 6.4 za konkretan prikaz danog prostog broja kao zbroja dva kvadrata.

Primjer 6.5. Zadan je $p = 113 = 4 \cdot 28 + 1$. Stoga, $p \mid a^2 + b^2$ za $a = \left(\frac{113-1}{2}\right)! = 56!$, $b = 1$. Kako je $56! \equiv 15 \pmod p$, slijedi da

$$p \mid 15^2 + 1^2$$

i $2p = 15^2 + 1^2$, odnosno $k = 2$, $x = 15$ i $y = 1$. Sada tražimo najmanje ostatke od x i y pri dijeljenju s k. To su očito $u = 1$, $v = 1$. Stavljamo

$$x_1 = \frac{xu + yv}{k} = 8, \; y_1 = \frac{xv - yu}{k} = 7$$

i dobivamo $113 = 8^2 + 7^2$.

Propozicija 6.6. *Prikaz prostog broja u obliku zbroja dva kvadrata, ako postoji, je jedinstven.*

Dokaz. Pretpostavimo da prost broj p možemo zapisati kao dva različita zbroja kvadrata, odnosno,

$$p = a^2 + b^2 = x^2 + y^2, \tag{6.5}$$

gdje su a i x, b i y iste parnosti. Iz (6.5) slijedi

$$a^2 - x^2 = y^2 - b^2,$$

odnosno

$$\frac{a-x}{2} \cdot \frac{a+x}{2} = \frac{y-b}{2} \cdot \frac{y+b}{2}. \tag{6.6}$$

Neka je $(\frac{a-x}{2}, \frac{y-b}{2}) = t$. Tada postoje $m, n \in \mathbb{Z}$, $(m, n) = 1$, za koje je

$$\frac{a-x}{2} = mt, \; \frac{y-b}{2} = nt.$$

Uvrštavanjem ovih jednakosti u (6.6) dobivamo:

$$mt \cdot \frac{a+x}{2} = nt \cdot \frac{y+b}{2},$$

odnosno

$$m \cdot \frac{a+x}{2} = n \cdot \frac{y+b}{2}.$$

Budući da su m i n relativno prosti, slijedi

$$\frac{a+x}{2} = nq, \ \frac{y+b}{2} = mq,$$

za $q \in \mathbb{Z}$. Sada je

$$a = \frac{a-x}{2} + \frac{a+x}{2} = mt + nq,$$

te

$$b = \frac{y+b}{2} - \frac{y-b}{2} = mq - nt.$$

Iz $p = a^2 + b^2$ i Diophantove relacije (6.1) slijedi

$$p = (mt+nq)^2 + (mq-nt)^2 = (m^2+n^2)(q^2+t^2)$$

što je u kontradikciji s time da je p prost broj. Dakle, prikaz prostog broja u obliku zbroja kvadrata, ako postoji, jest jedinstven. □

Sada možemo karakterizirati sve prirodne brojeve koji se mogu prikazati kao zbroj dva kvadrata. Na temelju Propozicije 6.1, Teorema 6.2 i relacije (6.1) možemo zaključiti sljedeću tvrdnju.

Teorem 6.7. *Prirodan broj n može se prikazati kao zbroj dva kvadrata ako i samo ako se u rastavu broja n na proste faktore svaki prosti faktor p za koji vrijedi da je* $p \equiv 3 \pmod 4$ *pojavljuje s parnom potencijom.*

6.2 Srodni problemi

Fermatovi rezultati o zbroju kvadrata potakli su istraživanja u nekoliko smjerova kako njega samog, tako i mnoge druge koji su došli iza njega.

Zbroj više kvadrata

Za početak, prirodno se pitati koji prirodni brojevi se mogu prikazati kao zbroj tri kvadrata. Fermat je dao kriterij za brojeve oblika $3k+1$. U konačnici su Legendre[2] i Gauss zaslužni za sljedeću tvrdnju:

Teorem 6.8 (Legendreov teorem o tri kvadrata)**.** *Prirodni broj n može se prikazati kao zbroj kvadrata tri cijela broja ako i samo ako n nije oblika* $4^a(8b+7)$ *za nenegativne cijele brojeve a i b.*

[2]Adrien-Marie Legendre (1752.-1833.), francuski matematičar

Prethodni teorem bio je iskorišten za dokaz tvrdnje da se svaki prirodan broj može prikazati kao zbroj četiri kvadrata. Još je u *Arithmetici* dano nekoliko primjera vezanih uz zbroj četiri kvadrata. Stoga se smatra da je Diophant bio svjestan teorema o zbroju četiri kvadrata. Bachet je 1621. godine u svom prijevodu *Arihtmetike* napisao da je uočio da se svaki prirodan broj može zapisati u obliku zbroja četiri kvadrata. Nadalje, napisao je da je tvrdnju provjerio za više od 300 brojeva te da ne zna kako ju dokazati. Euler ju je godinama pokušavao dokazati, no bezuspješno. On je pokušavao dokazati da se zadani broj može zapisati kao zbroj dva kvadrata s time da se i svaki od ta dva broja može također zapisati kao zbroj dva kvadrata. Tek 1770. godine Lagrange[3] je dao prvi dokaz. Iz tog razloga Teorem 6.9 zovemo još i Lagrangeov teorem o četiri kvadrata. Lagrange je priznao da mu je Eulerov rad o zbroju dva kvadrata uvelike pomogao u dokazivanju.

Teorem 6.9 (Teorem o četiri kvadrata)**.** *Svaki prirodan broj n može se prikazati u obliku zbroja četiri kvadrata, odnosno u obliku $n = a^2 + b^2 + c^2 + d^2$, za $a, b, c, d \in \mathbb{Z}$.*

Na primjer,

$$\begin{aligned} 5 &= 0^2 + 0^2 + 1^2 + 2^2, \\ 42 &= 0^2 + 1^2 + 4^2 + 5^2, \\ 78 &= 0^2 + 2^2 + 5^2 + 7^2, \\ 318 &= 2^2 + 3^2 + 4^2 + 17^2. \end{aligned}$$

Zbroj k-tih potencija

Poopćenje zbroja kvadrata je zbroj k-tih potencija. Odnosno, možemo pitati je li svaki prirodan broj prikaziv kao $n = x_1^k + \cdots + x_g^k$ pri čemu broj potencija u zbroju g ovisi samo o k, a ne ovisi o n, odnosno $g = g(k)$. Taj problem naziva se *Waringov problem*. Egzistenciju vrijednosti $g(k)$ dokazao je Hilbert[4] početkom 20. stoljeća. Danas je poznato da je $g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$.

Prosti brojevi oblika $x^2 + ny^2$

Fermat je proučavajući zbroj kvadrata zaključio da bi mogle vrijediti sljedeće tvrdnje:

- Svaki prost broj oblika $8n + 1$ ili $8n + 3$ može se prikazati kao $x^2 + 2y^2$.
- Svaki prost broj oblika $3n + 1$ može se prikazati kao $x^2 + 3y^2$.

[3]Joseph Louis Lagrange (1736.-1813.), talijanski matematičar i astronom

[4]David Hilbert (1862.-1943.), njemački matematičar

Ponovo ih je dokazao Euler. Sa slučajem $n = 5$, imao je problema. Još je i Fermat zaključio da je taj slučaj drugačiji nego slučajevi $n = 1, 2, 3$. Rješavanje tog problema, vodilo je Eulera do kvadratnog zakona reciprociteta. Općenito, problem reprezentacije brojeva u obliku $x^2 + ny^2$ pokazao se vrlo teškim problemom.

Binarne kvadratne forme

Jedno od važnijih tema u teoriji brojeva jesu binarne kvadratne forme, odnosno izrazi oblika $ax^2+bxy+yc^2$, gdje su a, b, cijeli brojevi. Za danu formu $ax^2+bxy+yc^2$, postavlja se problem određivanja svih cijelih brojeva n takvi da je $n = ax^2 + bxy + yc^2$ za neke $x, y \in \mathbb{Z}$. S tim, tzv. problemom reprezentacije bavili su se Lagrange i Gauss, a istraživanja različitih problema vezanih uz kvadratne forme traju još i danas.

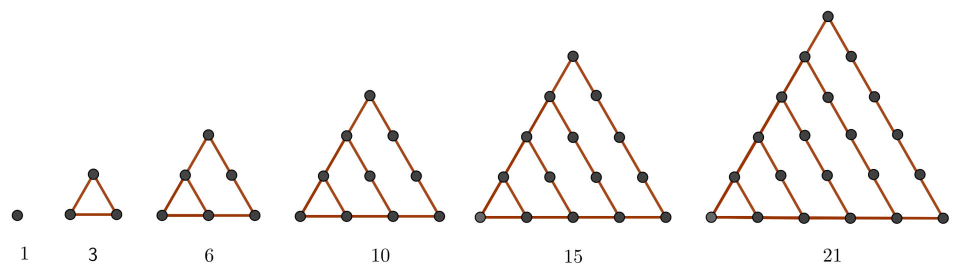
Poglavlje 7

Fermatov teorem o poligonalnim brojevima

7.1 Poligonalni brojevi

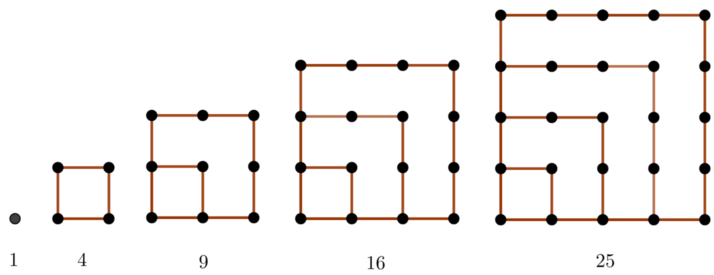
Figurativni brojevi dobivaju se slaganjem i preslagivanjem točkica u različite oblike. Njima su se bavili stari Grci, osobito Pitagorejci. *Poligonalni brojevi* formiraju pravilni geometrijski poligon.

Specijalno, brojevi koji čine istostranični trokut zovu se *trokutasti* ili *triangularni*. Generiramo ih kao na slici ispod:



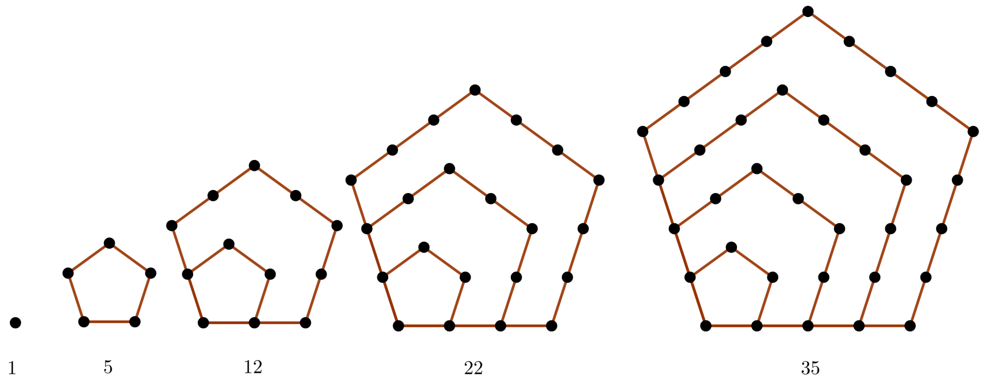
Trokutasti brojevi čine niz $1, 3, 6, 10, 15, \ldots$ čiji opći član je $\dfrac{n(n+1)}{2}$.

Kvadratne ili *tetragonalne* brojeve dobivamo pomoću sheme :



Kvadratni brojevi čine niz $1, 4, 9, 16, 25, \ldots$, odnosno (n^2).

Peterokutne ili *pentagonalne* brojeve predočavamo kao



Peterokutni brojevi su $1, 5, 12, 22, 35, \ldots$, odnosno $\left(\dfrac{n(3n-1)}{2}\right)$.

Definicija 7.1. *Neka su $n \geq 3$ i $k \geq 1$ prirodni brojevi.* Poligonalni brojevi *su prirodni brojevi oblika*

$$p(k, n) = \frac{(n-2)k^2 - (n-4)k}{2},$$

pri čemu $p(k, n)$ predstavlja k-ti element u nizu n-terokutnih brojeva.

Za $n = 3$ dobivamo trokutaste brojeve, $n = 4$ dobivamo kvadratne brojeve, itd.

7.2 Teorem o poligonalnim brojevima

Jedan od zanimljivih teorema vezanih uz poligonalne brojeve, konkretno uz kvadratne brojeve, je Lagrangeov teorem o četiri kvadrata 6.9. 1638. godine Fermat je naveo generalizaciju tog teorema, također bez dokaza. Uočio je da bi se svaki prirodan broj mogao zapisati kao zbroj najviše tri trokutasta broja, kao zbroj najviše četiri kvadratna broja, kao zbroj najviše pet peterokutnih brojeva itd.

Primjer 7.2. Broj 19 zapisan kao zbroj trokutastih, kvadratnih i peterokutnih brojeva:

$$19 = 1 + 3 + 5,$$

$$19 = 1 + 9 + 9,$$

$$19 = 1 + 1 + 5 + 12.$$

Teorem 7.3 (Fermatov teorem o poligonalnim brojevima)**.** *Svaki prirodan broj može se prikazati kao zbroj najviše n n-terokutnih brojeva.*

Lagrange i Gauss pokušavali su dokazati Fermatov teorem 7.3, no u tome nisu uspjeli. Lagrange je 1770. godine dokazao Fermatov teorem za $n = 4$, a Gauss je 1796. godine dokazao za n=3 (*Gaussov teorem o triagonalnim brojevima*). Postoji zanimljivost da je Gauss dokazavši teorem u svoj dnevnik zapisao "EYPHKA! num = $\triangle + \triangle + \triangle$". Zbog toga se taj teorem ponekad naziva i *Eureka teorem*.

Tek 1813. godine Cauchy[1] je prvi dao dokaz Teorema 7.3 što se smatra jednim od većih Cauchyevih doprinosa. Dokaz se bazira na lemi:

Lema 7.4 (Cauchyeva lema)**.** *Neka su a i b neparni prirodni brojevi takvi da $b^2 < 4a$ i $3a < b^2 + 2b + 4$. Tada postoje nenegativni cijeli brojevi s, t, u, v za koje vrijedi:*

$$a = s^2 + t^2 + u^2 + v^2, \tag{7.1}$$

$$b = s + t + u + v. \tag{7.2}$$

Dokaz. Kako su a i b neparni prirodni brojevi, slijedi da je $4a - b^2 \equiv 3 \pmod 8$. Stoga prema Gaussovom teoremu o trokutastim brojevima postoje neparni prirodni brojevi x, y, z, takvi da $0 < z \leq y \leq x$ i

$$4a - b^2 = x^2 + y^2 + z^2. \tag{7.3}$$

Odaberimo predznak $\pm z$ takav da vrijedi $b + x + y \pm z \equiv 0 \pmod 4$. Definirajmo s, t, u, v na sljedeći način:

$$s = \frac{b + x + y \pm z}{4},$$

[1]Augustin Louis Cauchy (1789.-1857.), francuski matematičar, inžinjer i fizičar

$$t = \frac{b+x}{2} - s = \frac{b+x-y\mp z}{4},$$
$$u = \frac{b+y}{2} - s = \frac{b-x+y\mp z}{4},$$
$$v = \frac{b\pm z}{2} - s = \frac{b-x-y\pm z}{4}.$$

Sada su jednakosti (7.1) i (7.2) zadovoljene i $v \le u \le t \le s$. Da bi pokazali da su ti brojevi nenegativni, dovoljno je pokazati da je $v \ge 0$, ili $v > -1$. To vrijedi ako je $b-x-y-z > -4$, odnosno ako je $x+y+z < b+4$. Maksimalnu vrijednost izraza $x+y+z$ dobivamo iz (7.3): $x+y+z \le \sqrt{12a-3b^2}$. Sada iz nejednakosti $3a < b^2+2b+4$ slijedi $x+y+z \le \sqrt{12a-3b^2} < b+4$. Time je tvrdnja dokazana. □

Poglavlje 8

Diofantske jednadžbe

Fermat je proučavao velik broj diofantskih jednadžbi. To su polinomijalne jednadžbe koje rješavamo u prstenu cijelih brojeva. Istaknut ćemo samo neke koje su danas poznate pod sljedećim nazivima:

1. Bachetova jednadžba
$$x^2 + k = y^3,$$
za $k \in \mathbb{Z}$,
2. Pellova jednadžba
$$x^2 - dy^2 = 1,$$
za $d \in \mathbb{N}$, d nije potpun kvadrat,
3. Pitagorina jednadžba
$$x^2 + y^2 = z^2,$$
4. Fermatova jednadžba
$$x^n + y^n = z^n,$$
za $n > 2$.

8.1 Bachetova jednadžba

Bachet je u svojem izdanju Diophantove *Arithmetike* izdane 1621. godine razmatrao jednadžbu oblika
$$x^2 + k = y^3, \tag{8.1}$$

gdje je $k \in \mathbb{Z}$ te je postavio pitanje njezine rješivosti. Fermat je proučavao dvije konkretne Bachetove jednadžbe: $x^2 + 2 = y^3$ i $x^2 + 4 = y^3$ te pronašao rješenja tih jednadžbi u skupu prirodnih brojeva:

$$(5, 3) \quad \text{rješenje jednadžbe} \quad x^2 + 2 = y^3 \tag{8.2}$$

te

$$(2, 2), (11, 5) \quad \text{rješenja jednadžbe} \quad x^2 + 4 = y^3. \tag{8.3}$$

Fermat je tvrdio da je ta rješenja pronašao pomoću svoje metode neprekidnog silaska. Lako se provjeri da su ta pozitivna rješenja zaista rješenja danih jednadžbi, no teško je za pokazati da su to jedina rješenja u skupu prirodnih brojeva. U skupu cijelih brojeva sva rješenja danih jednadžbi su:

$$(\pm 5, 3) \quad \text{rješenje jednadžbe} \quad x^2 + 2 = y^3, \tag{8.4}$$

te

$$(\pm 2, 2), (\pm 11, 5) \quad \text{rješenja jednadžbe} \quad x^2 + 4 = y^3. \tag{8.5}$$

Mordell[1] smatra da je upravo Bachetova jednadžba (8.1) odigrala temeljnu ulogu u razvoju teorije brojeva. Bachetova jednadžba proučava se više od 300 godina. Specijalne slučajeve riješili su poznati matematičari 18. i 19. stoljeća. Euler je predstavio novu ideju za rješavanje Bachetove jednadžbe za $k = 2$. Ta ideja sastojala se u tome da se faktorizira lijeva strana jednadžbe te da se dobije jednadžba

$$(x + \sqrt{2}i)(x - \sqrt{2}i) = y^3.$$

Rezultat je jednadžba čija je domena $D = \{a + b\sqrt{2}i : a, b \in \mathbb{Z}\}$. Ovdje su se prvi put u teoriji brojeva upotrebljavali kompleksni brojevi.

Dvadesetih godina prošlog stoljeća Mordell je pokazao da Bachetova jednadžba (8.1) ima konačno mnogo rješenja za svaki $k \in \mathbb{Z}$.

Šezdesetih godina prošlog stoljeća Baker[2] i Stark[3] su dali eksplicitne gornje granice za x i y u ovisnosti o broju k, što znači da se za dani k može pronaći rješenje jednadžbe, barem u teoriji. Nadalje, Bachetova jednadžba predstavlja važan primjer eliptičke krivulje koje su odigrale važnu ulogu u dokazu Velikog Fermatovog teorema.

8.2 Pellova jednadžba

Pellovu jednadžbu

$$x^2 - dy^2 = 1 \tag{8.6}$$

[1]Louis J. Mordell (1888.-1972.), američko-britanski matematičar

[2]Alan Baker (1939.-2018.), engleski matematičar, dobitnik Fieldsove medalje

[3]Harold Mead Stark (1939.-), američki matematičar

rješavamo u skupu prirodnih brojeva. Uočimo da u skupu cijelih brojeva uvijek ima rješenja $(\pm 1, 0)$, ali ona nam nisu od posebne važnosti. Nadalje, prepostavljamo da d nije potpun kvadrat jer bi u slučaju $d = a^2$ slijedilo

$$(x - ay)(x + ay) = 1,$$

odnosno $(x, y) = (\pm 1, 0)$.

Pellovom jednadžbom matematičari su se bavili stoljećima. Posebne slučajeve Pellove jednadžbe razmatrali su starogrčki matematičari (Theon Aleksandrijski[4], Arhimed[5]). Jedan od tih slučajeva je Pellova jednadžba

$$x^2 - 2y^2 = 1.$$

do koje su došli zbog problema aproksimacije broja $\sqrt{2}$. Indijski matematičar iz 7. st. Brahmagupta[6] je razvio metodu s kojom je mogao generirati beskonačno mnogo rješenja nekih Pellovih jednadžbi. U 12. stoljeću, Bhaskara II[7] opisao je prvu metodu za rješavanje opće Pellove jednadžbe. Metoda je ciklička i uvijek daje rješenje. Bhaskara je pomoću svoje metode riješio jednadžbu $x^2 - 61y^2 = 1$ i dobio najmanje rješenje u skupu prirodnih brojeva - $(1766319049, 226153980)$, što je bio fascinantan rezultat za ono doba.

Najmanje rješenje (x, y) u skupu prirodnih brojeva Pellove jednadžbe $x^2 - dy^2 = 1$, nazivamo *fundamentalno rješenje* te ga označavamo s (x_1, y_1) ili $x_1 + y_1\sqrt{d}$.

Prvi Europljani koji su pokazali interes za Pellovu jednadžbu bili su Fermat, Frenicle, Brouncker [8] i Wallis. Smatra se da je Fermat proučavajući jednadžbu (8.2) počeo proučavati jednadžbu (8.6) te je tako došao do tvrdnje sljedećeg teorema, ali bez dokaza.

Teorem 8.1. *Neka je d prirodan broj koji nije potpuni kvadrat. Jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja.*

Ukoliko je $(x_1, y_1) \in \mathbb{N}^2$ jedno rješenje (8.6), tada su sva rješenja dana s

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

za $n \in \mathbb{N}$. Lako se provjeri da (x_n, y_n) zaista zadovoljava jednadžbu. Naime, kako je

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n,$$

[4]Theon Aleksandrijski (oko 335.-oko 405.), grčki matematičar

[5]Arhimed (oko 287.pr.Kr.-212.pr.Kr.), grčki fizičar, astronom i matematičar

[6]Brahmagupta (598.-668.), indijski matematičar i astronom

[7]Bhaskara (1114.-1185.), indijski matematičar i astronom

[8]William Brouncker (1620.-1684.), engleski matematičar

množenjem izraza za $x_n + y_n\sqrt{d}$ i $x_n - y_n\sqrt{d}$ dobivamo

$$x_n^2 - y_n^2\sqrt{d} = (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n = (x_1^2 - y_1^2\sqrt{d})^n = 1.$$

Ono što nije tako očito jest činjenica da jednadžba (8.6) uvijek ima rješenje u skupu prirodnih brojeva. To se može pokazati pomoću tzv. Dirichletove leme:

Lema 8.2. *Ako je α iracionalan broj, onda postoji beskonačno mnogo relativno prostih cijelih brojeva p i q takvih da je $\left|\alpha - \frac{p}{g}\right| < \frac{1}{q^2}$.*

Nadalje, čak i kad znamo da rješenje postoji i da je sva rješenja moguće odrediti pomoću fundamentalnog, tj. najmanjeg rješenja, to najmanje rješenje može biti iznenađujuće veliko (kao npr. za $d = 61$). To je posebno intrigiralo i samog Fermata. Stoga on, u svojim pismima Bessyju, Wallisu, Brounckeru, kao izazov postavlja traženje fundamentalnog rješenja za neke konkretne vrijednosti broja d. Tako npr. Brouncker za $d = 313$ dobiva "ogromno" fundamentalno rješenje $(1819380158564160, 32188120829134849)$. Iako su Brouncker i Euler baratali s metodama koje dovode do fundamentalnog rješenja, one nisu bile dovoljno općenite. Metodu je u potpunosti razvio i usavršio Lagrange 1766. godine koristeći razvoj u verižni razlomak broja $\sqrt{d}$. Tek tada postaje jasno zašto za neke vrijednosti broja d dobivamo velika fundamentalna rješenja.

Veza između verižnog razlomka broja $\sqrt{d}$ i rješenja jednadžbe (8.6) je sljedeća:

Teorem 8.3. *Ako je $(u, v) \in \mathbb{N}^2$ rješenje Pellove jednadžbe(8.6), onda je $\frac{u}{v}$ konvergenta razvoja broja $\sqrt{d}$ u verižni razlomak.*

Štoviše, znamo precizno reći koje točno konvergente broja $\sqrt{d}$ predstavljaju rješenje:

Teorem 8.4. *Neka je r duljina perioda u razvoju od $\sqrt{d}$, te neka su $\left(\frac{p_n}{q_n}\right)$ konvergente. Ako je r paran sva rješenja jednadžbe (8.6) su*

$$(p_{nr-1}, q_{nr-1}),\ n \in \mathbb{N},$$

odnosno za n neparan

$$(p_{2nr-1}, q_{2nr-1}),\ n \in \mathbb{N}.$$

Nakon ovoga je lako otkriti razlog velikog fundamentalnog rješenja. Naime, duljina perioda u razvoju od $\sqrt{61}$ je čak 11 i k tome neparan broj, pa fundamentalno rješenje odgovara *velikoj* konvergenti (p_{21}, q_{21}) .

Za kraj, navodimo zanimljivost u vezi imena ove jednadžbe. Naime, unatoč postignućima mnogih drugih matematičara Pellova jednadžba nosi ime po engleskom matematičaru Johnu Pellu [9]. Naime, smatra se da je Euler zabunom nadjenuo ime Pellovoj jednadžbi pomiješajući postignuća Brounckera i Pella. 1658. godine J. Rahn [10] je objavio knjigu *Teutsche Algebra* koja sadrži primjere Pellove jednadžbe. U pisanju te knjige pomagao mu je J. Pell i to je jedina poveznica koja je pronađena između Pella i Pellove jednadžbe.

[9] John Pell (1611.-1685.), engleski matematičar i političar

[10] Johann Rahn (1622.-1676.), švicarski matematičar

Poglavlje 9

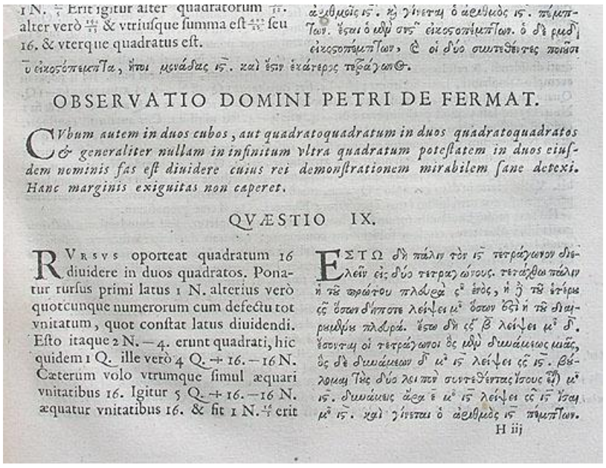
Veliki Fermatov teorem

Jedna od najpoznatijh Fermatovih slutnji, a danas i teorem, je sljedeća tvrdnja koja je zakotrljala lavinu matematičkih istraživanja i pridonijela razvoju algebarske teorije brojeva.

Teorem 9.1 (Veliki Fermatov teorem)**.** *Jednadžba*

$$x^n + y^n = z^n \tag{9.1}$$

nema rješenja u skupu prirodnih brojeva za $n > 2$.



1 N. Erit igitur alter quadratorum, alter verò & vtriusque summa est seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. erit

H iij

Slika 9.1: Observatio Domini Petri de Fermat

Priča u vezi ovog teorema započela je 1637. godine na margini Bachetovog prijevoda Diophantove *Arithmetike*. Tu je Fermat zapisao:

"Nije moguće kub rastaviti na dva kuba ili bikvadrat na dva bikvadrata niti općenitije neku potenciju veću od druge na dvije potencije s istim eksponentom. Za to imam stvarno čudesan dokaz, no rub je ovdje preuzak da ga zapišem."

Navodno je ovaj zapis pronađen posthumno. Original je izgubljen, a Fermatov sin Samuel izdao je 1670. godine Diophantovu Arithmetiku u koju je uključio očevu napomenu s margine naslovljenu s *Observatio Domini Petri de Fermat*.

Od objave ove tvrdnje do prvog uspješnog dokaza prošlo je točno 358 godina. 1994. godine dokaz je priveo Andrew Wiles[1] nakon višestoljetnog truda i doprinosa mnogih matematičara. Ne čudi stoga što ovaj teorem nosi ime i *Posljednji Fermatov teorem*, prema riječima G. Laméa iz prve polovice 19. stoljeća - *Od svih Fermatovih teorema o brojevima, samo je jedan ostao nepotpuno dokazan.*

Većina matematičara sumnja da je Fermat zaista imao dokaz ove tvrdnje. U svojoj prepisci s drugim matematičarima Fermat ih je upućivao da se usredotoče na dokaz te tvrdnje za $n = 3$ i $n = 4$. Moguće da je Fermat i imao neke dijelove dokaza za te specijalne slučajeve, osobito za slučaj $n = 4$. Zanimljivo je da je jedini objavljen Fermatov dokaz neke tvrdnje iz teorije brojeva bila baš tvrdnja vezana uz (9.1). Bila je to sljedeća propozicija.

Propozicija 9.2. *Neka su $a, b, c \in \mathbb{N}$ takvi da je $a^2 + b^2 = c^2$. Tada ne postoji $u \in \mathbb{N}$ takav da je $\frac{ab}{2} = u^2$.*

Drugim riječima prethodna tvrdnja kaže da *ne postoji Pitagorin trokut čija je površina potpun kvadrat.* Fermat ju je dokazao metodom silaska, a danas bi ju mogli jednostavno pokazati kao posljedicu od 9.1 za $n = 4$.

Dokaz Propozicije 9.2 metodom silaska. Neka je

$$a = 2st, b = s^2 - t^2, c = s^2 + t^2,$$

gdje su $s, t \in \mathbb{N}$, $s > t$, $(s, t) = 1$, odnosno kraće rečeno $(2st, s^2 - t^2, s^2 + t^2)$ je primitivna Pitagorina trojka. Nadalje, pretpostavljamo da je površina odgovarajućeg Pitagorinog trokuta potpun kvadrat,

$$P = \frac{ab}{2} = st(s + t)(s - t) = \square.$$

Faktori $s, t, s + t, s - t$ su u parovima relativno prosti i prema Propoziciji 5.2 svi su potpuni kvadrati. Stoga postoje $x, y, v, w \in \mathbb{N}$ za koje je:

$$s = x^2, t = y^2, s + t = w^2, s - t = v^2.$$

[1]Sir Andrew John Wiles (1953.-), britanski matematičar, dobitnik Abelove nagrade

Primijetimo da w i v moraju oba biti neparni i relativno prosti.

Promotrimo sada sljedeće razlike kvadrata:

$$x^2 - v^2 = s - (s - t) = t = y^2, \; w^2 - x^2 = (s + t) - s = t = y^2.$$

Slijedi da je $v^2 < x^2 < w^2$. Štoviše, vidimo da je $v^2 - x^2 = y^2 = w^2 - x^2$. Drugim riječima, x^2 je točno u sredini između v^2 i w^2. (Na primjer, kvadrat 169 je točno između kvadrata 49 i 289, tj. $49 < 169 < 289$.) Zaključujemo da je $w^2 - v^2 = 2y^2$, odnosno $2y^2 = (w - v)(w + v)$. Budući da su w i v neparni, slijedi da su $w + v$ i $w - v$ parni brojevi. Jedan od njih je tada djeljiv brojem 4, a drugi nije. (To je zato što se ta dva broja razlikuju za $2v$, a v je neparan broj i $2v = 2(2k + 1) = 4k + 2$.) Stoga je bilo koji od njih djeljiv s 4 te ga zapisujemo kao $4n^2$, a drugoga zapisujemo kao $2m^2$. Tada je

$$w = \frac{1}{2}((w + v) + (w - v)) = m^2 + 2n^2$$

i

$$v = \frac{1}{2}((w + v) - (w - v)) = \pm(m^2 - 2n^2),$$

pri čemu predznak broja v ovisi o tome koji broj je djeljiv brojem 4. Slijedi da je $2y^2 = (2m^2)(4n^2)$, odnosno $y = 2mn$.

Uočimo da smo došli do novog Pitagorinog trokuta sa katetama m^2 i $2n^2$:

$$\begin{aligned}(m^2)^2 + (2n^2)^2 = m^4 + 4n^4 &= \frac{1}{2}((m^2 + 2n^2)^2 + (m^2 - 2n^2)^2) \\ &= \frac{1}{2}(w^2 + (\pm v)^2) = \frac{1}{2}(w^2 + v^2) = x^2.\end{aligned}$$

Novi trokut čija je hipotenuza x je sigurno manji od početnog čija je hipotenuza $s^2 + t^2 = x^2 + y^2$. Također, površina novog trokuta je $P_1 = m^2 n^2$ što je potpun kvadrat. Dakle, sada smo dobili manji Pitagorin trokut čija je površina također potpuni kvadrat. Stoga prema metodi neprekidnog silaska zaključujemo da takav trokut ne postoji, odnosno da vrijedi tvrdnja propozicije. □

Dokaz Propozicije 9.2 kao posljedica VFT-a. Pretpostavimo da je $(a, b, c) \in \mathbb{N}^3$ i

$$a^2 + b^2 = c^2, \; 2ab = (2u)^2.$$

Sada je

$$(a + b)^2 - 2ab = (a + b)^2 - (2u)^2 = c^2,$$

odnosno

$$(a - b)^2 + 2ab = (a + b)^2 + (2u)^2 = c^2.$$

Množenjem posljednje dvije jednakosti dobivamo

$$(a + b)^4 - (2u)^4 = c^4,$$

što je u proturječju s Teoremom 9.1 za $n = 4$. □

Kroz sljedeća dva stoljeća matematičari su pokušavali dokazati ovaj teorem:

- 1660. godine Fermat dokazao slučaj $n = 4$ (?)
- 1753. godine Euler dokazao slučaj $n = 3$,
- 1825. godine, Legendre i Dirichlet[2] su nezavisno jedan od drugoga dokazali slučaj $n = 5$,
- 1839. godine Lamé[3] dokazao slučaj $n = 7$,
- 1849. godine Kummer[4] je dao dokaz za $n < 100$, $n \neq 37, 59, 67$,
- 1819. godine S. Germain[5] je pokazala da ako su p i $2p + 1$ prosti brojevi te p ne dijeli x, y, z, tada jednadžba (9.1) za $n = p$ nema rješenja u $\mathbb{N}$.
- 1983. godine G. Faltings [6] je dokazao da za svaki eksponent $n > 2$ postoji konačan broj trojki (x, y, z) u skupu prirodnih brojeva takvi da $(x, y, z) = 1$ i $x^n + y^n = z^n$.

Veliki Fermatov teorem bio je podijeljen na dva slučaja:

- $n \nmid xyz$,
- $n \mid xyz$.

Dokaz teorema za prvi slučaj dala je S. Germain, dok je dokaz za drugi slučaj puno teži. *Veliki Fermatov teorem* je najvjerojatnije bio najistaknutiji neriješen problem punih 360 godina. Tek 1993. godine Andrew Wiles, istraživač sa Sveučilišta Princeton, je prezentirao dokaz *Velikog Fermatovog teorema* tijekom izlaganja seminara na Sveučilištu u Cambridgeu. Isprva je Wilesu pronađena greška u dokazu, ali ju je kasnije uspio ispraviti. Dokaz je danas općenito prihvaćen, a prvi puta je objavljen u svibnju 1995. godine. Wiles je u svom dokazu koristio mnoga postignuća matematičara 17.-20. stoljeća u dokazivanju i opovrgavanju *Velikog Fermatovog teorema*. Wilesov dokaz je veoma složen te je za sada to jedini

[2]Johann Peter Gustav Lejeune Dirichlet (1805.-1859.), njemački matematičar
[3]Gabriel Lamé (1795.-1870.), francuski matematičar
[4]Ernst Kummer (1810.-1893.), njemački matematičar
[5]Sophie Germain (1776.-1831.), francuski matematičar, fizičar i filozof
[6]Gerd Faltings (1954.-), njemački matematičar

dokaz tog teorema, no mnogi i dalje pokušavaju pronaći jednostavniji dokaz. Ako takav dokaz ne postoji, onda se mogu potvrditi sumnje mnogih matematičara koji su smatrali da Fermat nikad nije imao općeniti dokaz.

Iako *Veliki Fermatov teorem* nema direktnu primjenu u teoriji brojeva, pokušaj dokazivanja teorema doveo je do snažnog razvoja teorije brojeva. Tako je u 19. stoljeću Kummer smatrao da ima dokaz *Velikog Fermatovog teorema*, no Dirichlet mu je ukazao na grešku u dokazu. Pokušavajući ispraviti grešku Kummer je razvio ideju o idealnim brojevima, koja je kasnije dovela Dedekinda[7] do definicije ideala, a što je pak dovelo do temeljnih algebarskih struktura (prsten, polje, domena jedinstvene faktorizacije i Dedekindova domena). Ovakav pristup razvio je podgranu teorije brojeva tzv. *algebarsku teoriju brojeva* koja je spoj algebre i teorije brojeva. U 20. stoljeću, bilo je evidentno da dokaz predstavlja dubok matematički problem. Na ideju se došlo da se originalan problem ekvivalentno zapiše kako problem na eliptičkoj krivulji i nakon doprinosa mnogih matematičara rezultiralo konačnim Wilesovim dokazom na oko 130 stranica, za što zasigurno margina knjige nije dovoljna.

[7] Julius Wilhelm Richard Dedekind (1831.-1916.), njemački matematičar

Bibliografija

[1] B. Dakić, *Figurativni brojevi*, https://mis.element.hr/fajli/176/31-05.pdf

[2] J. H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, Eighth edition, Cambridge University Press, 2008.

[3] L. E. Dickson, *History of the Theory of Numbers, Volume I: Divisibility and Primality*, Dover Publications, 2005.

[4] A. Dujella, *Sume kvadrata*, https://web.math.pmf.unizg.hr/~duje/utb/sumekvadrata2.pdf

[5] A. Dujella, *Uvod u teoriju brojeva*, skripta, https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf

[6] H. M. Edwards, *Fermat's Last Theorem*, Springer-Verlag, New York, 2000.

[7] Z. Franušić, *Pellova jednadžba*, nastavni materijal, https://web.math.pmf.unizg.hr/nastava/etb/materijali/pellova-web.pdf

[8] I. Kleiner, *Excursions in the History of Mathematics*, Birkhäuser Basel, 2012.

[9] M. Křižek, F. Luca, L. Somer *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, Springer, 2001.

[10] M. B. Nathason *A short proof od Cauchy's polygonal number theorem*, https://www.ams.org/journals/proc/1987-099-01/S0002-9939-1987-0866422-3/S0002-9939-1987-0866422-3.pdf.

[11] W. Scharlau, H. Opolka, *From Fermat to Minkovski*, Springer-Verlag, 1984.

[12] *Bachet de Méziriac, Claude-Gaspar (1581-1638)*, http://www.daviddarling.info/encyclopedia/B/Bachet.html

[13] *Fermat's little theorem*, https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

[14] *Fermat's Method of Infinite Descent*, https://brilliant.org/wiki/general-diophantine-equations-fermats-method-of/

[15] *Fermat number*, https://en.wikipedia.org/wiki/Fermat_number

[16] *Fermat polygonal number theorem*, https://en.wikipedia.org/wiki/Fermat_polygonal_number_theorem

[17] *Number Theory Begins*, http://assets.press.princeton.edu/chapters/s10165.pdf

[18] *Pierre de Fermat*, https://en.wikipedia.org/wiki/Pierre_de_Fermat

[19] *Proofs of Fermat's theorem on sums of two squares*, https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_theorem_on_sums_of_two_squares#Zagier's_%22one-sentence_proof%22

Sažetak

Pierre de Fermat jedan je od najvećih matematičara 17. stoljeća. Smatra ga se utemeljiteljem moderne teorije brojava. Glavni cilj ovog diplomskog rada je prikazati i dijelom dokazati Fermatove rezultate i doprinose u teoriji brojeva. Fermat je dao čitav niz tvrdnji, uglavnom bez dokaza, koje su se godinama, a neke i stoljećima kasnije pokazale istinitima. Fermat je poznat po brojevima oblika $F_m = 2^{2^m} + 1, m \in \mathbb{N}$ koji se zovu *Fermatovi brojevi* te po svom doprinosu u razvoju diofantskih jednadžbi. U radu su iskazani i dokazani (svi osim posljednjeg) Fermatovi teoremi: *Mali Fermatov teorem, Teorem o zbroju dva kvadrata, Teorem o poligonalnim brojevima* i *Veliki Fermatov teorem*. Osim teorema u radu su opisane i na primjerima objašnjene dvije Fermatove metode: *Fermatova metoda faktorizacije* i *Fermatova metoda neprekidnih silazaka*.

Summary

Pierre de Fermat is one of the greatest mathematicians of 17. century. He is considered a founder of modern number theory. The main purpose of this work is to present and partly to prove the results and contributions Fermat's contributions to number theory. Fermat gave a whole series of assertions, mostly without the proof, which have been years, and some of them centuries later proved to be true. Fermat is famous for his numbers $F_m = 2^{2^m} + 1, m \in \mathbb{N}$, which we call Fermat's numbers, and for his contributions in development of Diophant's equations. In the work are presented and proved (all except the last one) following theorems: *Fermat's Little theorem, Two-Square Theorem, Fermat polygonal number theorem* and *Fermat's Last Theorem*. Except the theorems, two Fermat's methods: *Fermat's factorizations method* and *Fermat's method of infinite descent* are described and explained trough the examples.

Životopis

Rođena sam 04.10.1994. godine u Varaždinu. U razdoblju od 2001./2002. do 2008./2009. pohađala sam Osnovnu školu "Metel Ožegović" Radovan. Zatim sam svoje školovanje nastavila od 2009./2010. do 2012./2013. u Drugoj gimnaziji u Varaždinu.
Akademske godine 2013./2014. sam upisala Prirodoslovno - matematički fakultet u Zagrebu, preddiplomski studij, matematika, nastavnički smjer. Ovaj studij sam završila u roku od tri godine, bez zaostajanja i ponavljanja, te sam stekla titulu sveučilišnog prvostupnika edukacije matematike.
Zatim sam akademske godine 2016./2017. upisala diplomski studij, matematika, nastavnički smjer na istoimenom fakultetu.
Osim matematičkog znanja, tijekom svog školovanja stekla sam informatičku pismenost te sam ovladala engleskim jezikom.